PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-231776

(43)Date of publication of application : 27.08.1999

(51)Int.Cl. G09C 1/00
G09C 1/00
H04L 9/32

(21)Application number : 10-031560

(22)Date of filing : 13.02.1998

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(72)Inventor : SHIMADA MASAKAZU
TOKUNAGA HIDETOSHI
HOSHIKO TAKAYUKI
YASUDA HITOSHI

(54) METHOD AND DEVICE FOR ISSUING CERTIFICATE

(57)Abstract:

PROBLEM TO BE SOLVED: To confirm identity online and to issue a certificate certifying the public key of that person.

SOLUTION: Certificate application information CRI contains secret information showing the identity such as a credit number, this CRI is made into CRI-S by adding a digital signature through a disposable secret key Ss1, this is enciphered into CRI-S-E by a random generation cryptographic key Er, a shared key SK is prepared by the disposable secret key Ss1 and a public key Ep of an application accepting device, Er is enciphered into Er-E by the SK and CRI-S- E, Er-E, public key Sp1 of the Ss1 and public key Ep1 of the Es1 are sent to the application accepting device. At the accepting device, the SK is prepared by the secret keys Es2 and Ep1, the Er-E is deciphered by the SK, the CRI-S-E is deciphered by the Er and CRI-S is verified by the Sp1. In the case of successing, the legality of the secret information showing the identity in the CRI is confirmed and a certificate is issued.

LEGAL STATUS

[Date of request for examination] 14.12.2000

[Date of sending the examiner's decision of rejection] 14.09.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] Generally certificate application equipment creates certificate application information including the information which only he cannot know. Furthermore, generate a disposable key and security-ization of the above-mentioned certificate application information is performed using the disposable key. The above-mentioned disposable key, the disposable public key information that a pair is made, and the information security-ized [above] to certificate application acceptance equipment Then, delivery, Certificate application acceptance equipment verifies the information security-ized [above] using disposable public key information, and to certificate issue equipment, if the above-mentioned verification result is success, delivery and the above-mentioned certificate issue equipment the verification result And it is the certificate issue approach which does not perform issue of a certificate when a certificate is published and justification cannot be checked, if the justification of certificate application information is checked and the justification is checked, but is characterized by certificate issue equipment notifying the result of certificate issue procedure to certificate application equipment.
[Claim 2] the above-mentioned disposable key -- dispersion -- a logarithm -- with the private key in a system unsymmetrical key cipher system, and the disposable key for key delivery which consists of a pair of a public key It is the disposable key for digital signatures which consists of a pair of a private key and a public key, and disposable public key information is the above-mentioned disposable public key for key delivery, and the above-mentioned disposable public key for digital signatures. Security-ization of the above-mentioned certificate application information performs a digital signature with the disposable private key for digital signatures to the above-mentioned certificate application information. And it is enciphering the certificate application information with a signature with the key for encryption generated at random, and acquiring security-ized certificate application information. A share key is generated using the above-mentioned disposable private key for key delivery, and the public key for key delivery of the above-mentioned certificate application acceptance equipment, the above-mentioned key for encryption is enciphered with the above-mentioned share key, and the encryption information on an encryption key is generated. The above-mentioned security-ized certificate application information, The encryption information on the above-mentioned encryption key is added to the above-mentioned disposable public key information, and it considers as certificate application demand information. To the above-mentioned application acceptance equipment verification of delivery and the information security-ized [above] The above-mentioned beam above-mentioned certificate application demand information with a receptacle is divided into the encryption information and disposable public key information on the key for security-ized certificate application information encryption. A share key is generated using the above-mentioned disposable public key for key delivery, and the private key for key delivery of the certificate application acceptance equipment. Decrypt the encryption information on the above-mentioned key for encryption with the share key, decode security-ized certificate application information with the above-mentioned share key, and certificate application information and a digital signature are acquired. The certificate issue approach according to claim 1 characterized by being verifying certificate application information using the above-mentioned disposable public key for digital signatures.

[Claim 3] the above-mentioned disposable key -- dispersion -- a logarithm -- with the private key in a system unsymmetrical key cipher system, and the disposable key for key delivery which consists of a pair of a public key It is the disposable key for digital signatures which consists of a pair of a private key and a public key. The above-mentioned disposable public key information They are the above-mentioned disposable public key for key delivery, and the above-mentioned disposable public key for digital signatures. A share key is generated using the above-mentioned disposable private key for key delivery, and the public key for key delivery of the above-mentioned certificate application acceptance equipment. Security-ization of the above-mentioned certificate application information The above-mentioned disposable private key for digital signatures performs a digital signature to the above-mentioned certificate application information. And verification of the information which is enciphering this certificate application information with a signature with the above-mentioned share key, and acquiring security-ized certificate application information, and was security-ized [above] The security-ized certificate application information and disposable public key information which were received are divided. Generate a share key using the disposable public key for key delivery and the private key for key delivery of certificate acceptance equipment in the above-mentioned public key information, and the above-mentioned security-ized certificate application information is decrypted with the share key. The certificate issue approach according to claim 1 characterized by being acquiring certificate application information with a signature and carrying out signature verification of this certificate application information with a signature using the disposable public key for a signature in the above-mentioned public key information.

[Claim 4] A means to create certificate application information including the user information which has the extra sensitive information which shows this human nature, user key information, etc., a means to generate the disposable private key and public key for digital signatures, and dispersion -- a logarithm -- with a means to generate the disposable private key and public key for key delivery in a system unsymmetrical key cipher system A means to generate the key for encryption at random, and a means to generate a share key using the private key of throwing away for [above-mentioned] key delivery, and the public key for key delivery of certificate application acceptance equipment, A means to perform a digital signature for the above-mentioned certificate application information using the above-mentioned disposable private key for digital signatures, A means to encipher the above-mentioned digital office naming certificate application information with the above-mentioned encryption key, and to generate security-ized certificate application information, A means to acquire the encryption key information enciphered by enciphering the above-mentioned encryption key with the above-mentioned common key, The above-mentioned security-ized certificate application information and the encryption key information by which encryption was carried out [above-mentioned], A means to transmit the above-mentioned disposable public key for digital signatures, and the above-mentioned disposable public key for key delivery to the above-mentioned certificate application acceptance equipment, Certificate application equipment possessing the control means which performs R/W of as opposed to a storage means in making each above-mentioned means process sequentially **** etc., and an above-mentioned storage means to memorize information required for the above-mentioned processing.

[Claim 5] A means to create certificate application information including the user information which has the extra sensitive information which shows this human nature, user key information, etc., a means to generate the disposable private key and public key for digital signatures, and dispersion -- a logarithm -- with a means to generate the disposable private key and public key for key delivery in a system unsymmetrical key cipher system A means to generate a share key using the private key of throwing away for [above-mentioned] key delivery, and the public key for key delivery of certificate application acceptance equipment, A means to perform a digital signature for the above-mentioned certificate application information using the above-mentioned disposable private key for digital signatures, A means to encipher the above-mentioned digital office naming certificate application information with the above-mentioned share key, and to generate security-ized certificate application information, The above-

mentioned security-ized certificate application information and the above-mentioned disposable public key for digital signatures, Certificate application equipment possessing a means to transmit the above-mentioned disposable public key for key delivery to the above-mentioned certificate application acceptance equipment, the control means which performs R/W of as opposed to a storage means in making each above-mentioned means process sequentially **** etc., and an above-mentioned storage means to memorize information required for the above-mentioned processing.

[Claim 6] A means to generate the private key for key delivery, and a means to receive the certificate application demand information from certificate application equipment, The received certificate application demand information Security-ized certificate application information, The enciphered encryption key information and the disposable public key for digital signatures, A means to generate a share key using a means to divide into the disposable public key for key delivery, and the above-mentioned private key and the above-mentioned disposable public key for key delivery, A means to decrypt the encryption key information by which encryption was carried out [above-mentioned] with the above-mentioned share key, and to obtain an encryption key, A means to decrypt the above-mentioned security-ized certificate application information with the above-mentioned encryption key, and to acquire digital office naming certificate application information, A means to verify certificate application information for the above-mentioned digital office naming certificate application information using the above-mentioned disposable public key for digital signatures, Certificate application acceptance equipment possessing the control means which is made to process each above-mentioned means sequentially, and performs the R/W to a storage means etc., and an above-mentioned storage means to memorize information required for the above-mentioned processing.

[Claim 7] A means to generate the private key for key delivery, and a means to receive the certificate application demand information from certificate application equipment, The received certificate application demand information Security-ized certificate application information, A means to divide into the disposable public key for digital signatures, and the disposable public key for key delivery, A means to generate a share key using the above-mentioned private key and the above-mentioned disposable public key for key delivery, A means to decrypt the above-mentioned security-ized certificate application information with the above-mentioned share key, and to acquire digital office naming certificate application information, A means to verify certificate application information for the above-mentioned digital office naming certificate application information using the above-mentioned disposable public key for digital signatures, Certificate application acceptance equipment possessing the control means which is made to process each above-mentioned means sequentially, and performs the R/W to a storage means etc., and an above-mentioned storage means to memorize information required for the above-mentioned processing.

[Claim 8] Certificate application information acceptance equipment according to claim 6 or 7 characterized by having a means to verify the justification from the extra sensitive information which shows this human nature in the above-mentioned certificate application information if the above-mentioned signature verification is passed, and a means to publish the certificate according to the application information if verification of the justification is passed.

[Translation done.]

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the method of applying for an electronic certificate, verifying this using a telecommunication system, a computer, etc., and publishing a certificate, and its equipment.
[0002]
[Description of the Prior Art] It is possible to acquire various kinds of electronic intelligence, such as various program data and data of various databases. In this case, using the public key in a receipt and its certificate, a data feeder enciphers supply data, and offers the certificate in which it is shown that it is his thing of a public key, and it enables it to decode that supplied encryption data with the private key which only that user holds secretly so that the data to supply may not be acquired by the 3rd person.
[0003] in order to have such a certificate published and to check this human nature of a certificate applicant in the former -- him in off-line -- the need of attesting existed. therefore, automation and increase in efficiency are restricted and the processing takes ****** in **, and cost. trustworthy him to whom security was secured, without having solved the above problems and revealing individual humanity news -- the technique in which authentication is realized is not established.
[0004]
[Problem(s) to be Solved by the Invention] him in off-line -- while it has the same safety as authentication -- him -- it is offering the method of realizing increase in efficiency and real time-ization of certificate application / issue processing by online-izing of authentication, and its equipment. him in the online in a certificate application and issue although the above-mentioned conventional technique also described -- the technique which realized authentication is not established.
[0005] In order to perform he authentication, it is necessary to show the information (or object) which only he cannot have. the electronic world -- him -- although a digital signature method exists as a technique for realizing authentication, a digital signature method is realized on the credit of a key. It is difficult to attest this human nature of those who do not hold the key by which the credit was carried out. therefore, the time of receiving the credit of a key for the first time with the conventional technique -- him in off-line -- authentication was needed and the problem existed in a cost side, convenience, etc. Although what is necessary is just to show the information which only he cannot know to the partner who wants to receive authentication in order to attest this human nature on-line from the condition that the credit of a key is not carried out, the threat of the information being revealed to a third person exists in that case. if the information which only he cannot know can transmit where security is secured -- him in online -- authentication also becomes possible.
[0006] The purpose of this invention offers the certificate issue approach that a certificate applicant and a certificate publisher can carry out certificate application / issue processing efficiently on-line. Another purpose of this invention is to offer the certificate issue approach that a certificate issue engine system can be carried out by low cost. Still more nearly another purpose of this invention is to offer the certificate issue approach that safe certificate issue processing which eliminated the threat of spoofing by the third person can be carried out.
[0007]
[Means for Solving the Problem] Transmission and reception of the information for attesting are enabled. the certificate issue approach of this invention introduces the new concept of a disposable key --

insurance -- him -- The information to which a certificate applicant cannot know only an applicant to a certificate publisher, for example, he, is the member of credit finance. In the condition that the credit of a key is not carried out by showing insurance the name of the credit number which only he and a credit firm cannot know, and him, the address, etc., authentication of this positive human nature in online is guaranteed, and operation of positive certificate issue is enabled.

[0008] Processing of the certificate issue approach is carried out at the following steps.

Step 1: Generally a certificate applicant inputs certificate application information including the information which only he cannot know to certificate application equipment.

Step 2: Certificate application equipment generates a disposable key and performs security-ization of certificate application information using it.

Step 3: Certificate application equipment sends the above-mentioned disposable key, the disposable public key information that a pair is made, and the information security-ized at step 2 to certificate application acceptance equipment.

Step 4: Certificate application acceptance equipment verifies the information security-ized using disposable public key information, and sends a verification result to certificate issue equipment.

Step 5: Certificate issue equipment opts for the handling of certificate application information according to a verification result.

Step 6: Certificate issue equipment publishes a certificate, when the justification of certificate application information is checked, and issue of a certificate is not performed when justification cannot be checked.

Step 7: Certificate issue equipment notifies the result of certificate issue procedure to an applicant.

[0009]

[Embodiment of the Invention] Hereafter, the example of this invention is explained in detail using a drawing. The example of the system configuration by which the approach of this invention is applied to drawing 1 is shown. Using certificate application equipment 11, a certificate applicant makes certificate application information and sends to the certificate application acceptance equipment 14 in the certificate authority equipment 13 connected by the communication line 12. Certificate application acceptance equipment 14 verifies receipt information, and sends the verification result and certificate application information to certificate issue equipment 15. Certificate issue equipment 15 sends the verification result and the result of having responded to verification of certificate application information to certificate application equipment 11 through a communication line 12.

[0010] The example of a functional configuration of certificate application equipment 11 is shown in drawing 2 . To the application information generation section 21, the key generation section 22 for a signature, the key generation section 23 for delivery, the common key generation section 24, the encryption key generation section 25, the signature section 26, the encryption sections 27 and 28, the public key transmit information generation section 29, the bond part 31 that combines the information which should be sent out, and the exterior, information It consists of input means 36, such as a keyboard which inputs the control section 35 which controls the transmitting section 32 which transmits, the receive section 33 which receives the information from the outside, the storage section 34 which memorizes various information, and each part sequentially, or performs the R/W to the storage section 34, various information, a command, etc., etc. These are usually constituted by the microprocessor etc.

[0011] Each example of a functional configuration of certificate application acceptance equipment 14 and certificate issue equipment 15 is shown in drawing 3 . With certificate application acceptance equipment 14, the receive section 41 which receives the information from the outside, the division section 42 which divides the received information, the key generation section 43 for delivery, the common key generation section 44, the decryption sections 45 and 46, the signature verification section 47, the storage section 48 that memorizes various information, and each part are controlled sequentially, or it has the control section 49 which performs the R/W to the storage section 48 etc.

[0012] Certificate issue equipment 15 is equipped with the justification verification section 51, the

certificate issue section 52, and the transmitting section 53 that sends out information to the exterior. When certificate application acceptance equipment 14 and certificate issue equipment 15 are separated regarding the place, information is prepared for **, the transmitting section which carries out a carrier, and a receive section in between [these], respectively. Next, the procedure of a certificate application is explained with reference to drawing 2 thru/or drawing 4 . The certificate application receiving set 14 which the certificate applicant operated certificate application equipment 11, charged the disposable public key Ep2 for key delivery to the certificate application receiving set 14, and received this claim The disposable private key Es2 for delivery and a public key Ep2 are generated in the key generation section 43 for delivery, and while storing temporarily the private key Es2 in the storage section 48, it sends to certificate application equipment 11 through the transmitting section 53 of certificate issue equipment 15. Certificate application equipment 11 stores temporarily the disposable public key Ep2 for delivery of the received certificate application acceptance equipment 14 in the storage section 34. these keys Es2 and Ep2 for key delivery -- dispersion -- a logarithm -- it is used for a system unsymmetrical key cipher system.

[0013] previously -- certificate application equipment 11 -- actuation of an applicant -- a basis -- **** and user information -- The certificate application information CRI which consists of user key information etc. is built in the application information generation section 21 (S1). A private key Es1 and a public key Ep1 are generated in the key generation section 23 for delivery as a disposable key for key delivery (S2), and a private key Ss1 and a public key Sp1 are generated in the key generation section 22 for a signature as a disposable key for digital signatures (S3). The key in a factorization-in-prime-numbers system unsymmetrical key cipher system and the key in other cipher systems are sufficient as these disposable keys Ss1 and Sp1 for a signature.

[0014] The information (for example, credit code) as which the confidentiality which shows this human nature is required is also included in the certificate application information CRI. The disposable key for key delivery has the following relation.

Ep1=Es1andG [p]

G [p] is a open parameter here. that is, this key -- dispersion -- a logarithm -- it is used for a system unsymmetrical key cipher system.

[0015] Certificate application equipment 11 uses a private key Ss1 for the certificate application information CRI, performs electronic signature in the signature section 26, and generates digital office naming certificate application information CRI-S (S4). On the other hand, it is the encryption key generation section 25 to the key Er for encryption. It generates at random (S5), and it enciphers in the encryption section 27 to certificate application information CRI-S with a signature using this, and security-ized certificate application information CRI-S-E is generated (S6).

[0016] moreover, the object for key delivery -- share key SK=Es-1 and Ep-2 are generated in the common key generation section 24 using public key Ep-2 of disposable private key Es-1 and certificate application acceptance equipment 14 (S7). This share key SK has the relation between SK=Es-2 and Ep-1. This share key SK is used and it is the key Er for encryption at the encryption section 28. It enciphers and encryption information Er-E of an encryption key is obtained (S8).

[0017] The public key transmit information DPI for throwing away containing public key Sp-1 and Ep-1 is generated in the public key transmit information generation section 29 (S9). This information DPI is good at mere bit-connecting DPI=Sp-1 ||Ep-1 of Sp-1 and Ep-1. Bit connecting of DPI is carried out to CRI-S-E and Er-E by the bond part 31, the certificate application demand information SCRI is generated (S10), and this application demand information SCRI is transmitted to certificate application acceptance equipment 14 from the transmitting section 32 (S11).

[0018] The application demand information SCRI fills the following relational expression.

SCRI=DPI||CRI-S-E||Er-E =DPI||(enc (Er:CRI-S)) || (enc (SK:Er))

= DPI||(enc (Er:sig (Ss-1:CRI))) || (enc (SK:Er))

|| means connection here, it means that enc (A:B) enciphers B using Key A, and sig (A:B) means carrying

out signature grant of the B using Key A.
The certificate application acceptance equipment / issue equipment operations sequence concerning one example of invention of certificate verification / ****** are shown in drawing 5 .
[0019] Certificate application acceptance equipment 14 divides into DPI, CRI-S-E, and Er-E the application demand information SCRI received in the receive section 41 in the division section 41 (S1). SpI and EpI are obtained from the DPI. the object for encryption of the Sp-1 and certificate application acceptance equipment 14 -- the share key SK is generated in the share key generation section 44 using private key Ss-2 (S2). That is, SK=Es2 and Ep1 are calculated in the share key generation section 44. The share key SK generated with certificate application acceptance equipment 14 and the share key SK generated with certificate application equipment 11 are the same.
[0020] Er-E is decrypted in the decryption section 45 using the generated share key SK, and it is the encryption key Er. It obtains (S3). The encryption key Er CRI-S-E is decrypted in the decryption section 46, and CRI-S is obtained (S4). CRI-S is verified using Sp1 in DPI in the signature verification section 47 (S5). When the verification result is unusual, since existence of threats, such as an alteration, is clear, the purport that certificate registration was stopped and registration was un-completing is shown to certificate application equipment 11 through the transmitting section 53 from the certificate issue section 52 (S6).
[0021] When the justification of CRI is guaranteed by the signature verification result, the information as which the confidentiality which shows this human nature is demanded, for example, a credit number, is acquired from CRI, and this human nature is checked in the justification verification section 51 using the information (S7). It is got blocked, for example, confirms whether to be what he has [the credit number]. When this human nature is checked, a certificate is published in the certificate issue section 52, and the transmitting section 53 shows certificate application equipment 11 the purport which certificate issue processing ended normally (S8). When this human nature cannot be checked, the purport to which certificate issue processing was stopped and certificate issue was not carried out is shown to certificate application equipment 11 through the transmitting section 53 in the certificate issue section 52 (S6).
[0022] It sets to **** and is the encryption key Er. Although it was made to generate at random and certificate application information signature CRI-S was enciphered, as a broken line shows in drawing 2 , it is this encryption key Er. CRI-S may be instead enciphered with the share key SK. In this case, the encryption key generation section 25 and the encryption section 28 are omitted by drawing 2 , therefore CRI-S-E and DPI are seen off in certificate application acceptance equipment 14, and Er-E is omitted. The decryption to CRI-S-E is performed in the decryption section 46 by the share key SK which the decryption section 45 was omitted with certificate application acceptance equipment 14, and was generated in the share key generation section 44. Certificate application acceptance equipment may serve as certificate issue equipment in ****.
[0023]
[Effect of the Invention] As stated above, in this invention, reservation of security is realized to the guarantee of this human nature by introducing the new concept of a disposable key by including the extra sensitive information which shows this human nature which only he can know again in certificate application information. Furthermore, the burden of certificate application equipment and certificate issue equipment is also mitigated, and there is also little system cost about certificate issue processing.
[0024] Moreover, the threat of spoofing by the third person is prevented and safe certificate issue processing can be realized.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] The block diagram showing the example of the structure of a system to which this invention approach is applied.
[Drawing 2] The block diagram showing the functional configuration of the example of the certificate application equipment by this invention.
[Drawing 3] The block diagram showing the functional configuration of the example of the certificate application acceptance equipment by this invention.
[Drawing 4] The flow chart showing the example of the operations sequence of the certificate application equipment shown in drawing 2 .
[Drawing 5] The flow chart showing the example of the operations sequence of the certificate application acceptance equipment shown in drawing 3 .

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－231776

(43)公開日　平成11年(1999)８月27日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ
			６４０Ｚ
	６６０		６６０Ｇ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｄ

審査請求　未請求　請求項の数８　ＯＬ　（全７頁）

(21)出願番号　特願平10－31560

(22)出願日　平成10年(1998)２月13日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号
(72)発明者　島田　昌和
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　徳永　秀俊
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　星子　隆幸
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　弁理士　草野　卓

最終頁に続く

(54)【発明の名称】　証明書発行方法およびその装置

(57)【要約】
【課題】　オンラインで本人性を確認し、その人のその公開鍵であることの証明書を発行する。
【解決手段】　証明書申請情報ＣＲＩに、クレジット番号のような本人性を示す機密情報を含め、このＣＲＩを使い捨て秘密鍵Ｓｓ１でディジタル署名を付けＣＲＩ－Ｓとし、これをランダム生成暗号鍵Ｅｒ で暗号化してＣＲＩ－Ｓ－Ｅとし、使い捨て秘密鍵Ｅｓ１と申請受理装置の公開鍵Ｅｐで共有鍵ＳＫを作り、ＳＫでＥｒ を暗号化してＥｒ －Ｅとし、ＣＲＩ－Ｓ－Ｅ、Ｅｒ －Ｅ、Ｓｓ１の公開鍵Ｓｐ１、Ｅｓ１の公開鍵Ｅｐ１を申請受理装置へ送る。受理装置は、秘密鍵Ｅｓ２とＥｐ１でＳＫを作り、ＳＫでＥｒ －Ｅを復号し、Ｅｒ でＣＲＩ－Ｓ－Ｅを復号し、ＣＲＩ－ＳをＳｐ１で検証し、合格するとＣＲＩ中の本人性を示す機密情報の正当性を確認して証明書を発行する。

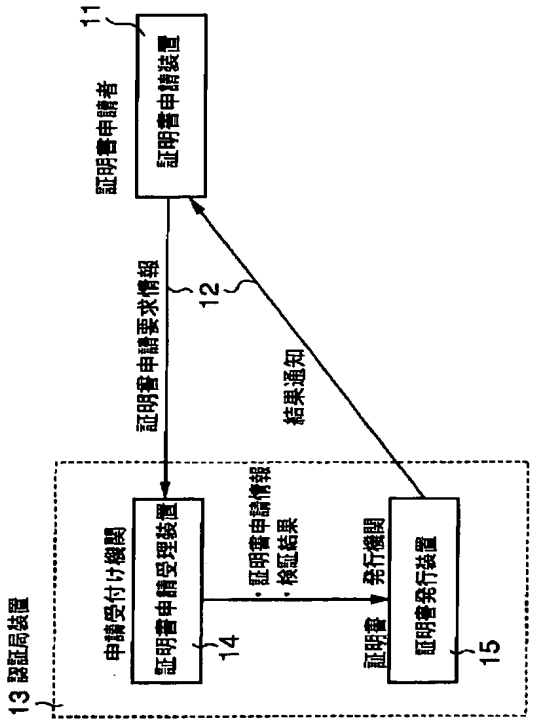

図１

1

【特許請求の範囲】

【請求項１】　証明書申請装置は、一般には本人しか知り得ない情報を含む、証明書申請情報を作成し、
更に使い捨て鍵を生成し、
その使い捨て鍵を用い、上記証明書申請情報のセキュリティ化を行い、
その後、上記使い捨て鍵と対をなす使い捨て公開鍵情報と上記セキュリティ化した情報を証明書申請受理装置に送り、
証明書申請受理装置は使い捨て公開鍵情報を用い上記セキュリティ化された情報を検証し、
その検証結果を証明書発行装置に送り、
上記証明書発行装置は上記検証結果が合格であれば、かつ証明書申請情報の正当性を確認し、
その正当性が確認されると証明書の発行を行い、正当性を確認できない場合は証明書の発行は行わず、
証明書発行装置は証明書発行手続きの結果を証明書申請装置に対し通知することを特徴とする証明書発行方法。

【請求項２】　上記使い捨て鍵は離散対数系非対称鍵暗号方式における秘密鍵、公開鍵の対からなる鍵配送用使い捨て鍵と、秘密鍵と公開鍵の対からなるディジタル署名用使い捨て鍵であり、
使い捨て公開鍵情報は上記鍵配送用使い捨て公開鍵および上記ディジタル署名用使い捨て公開鍵であり、
上記証明書申請情報のセキュリティ化は上記証明書申請情報に対してディジタル署名用使い捨て秘密鍵でディジタル署名を行い、かつランダムに生成した暗号化用鍵でその署名付証明書申請情報を暗号化してセキュリティ化証明書申請情報を得ることであり、
上記鍵配送用使い捨て秘密鍵と上記証明書申請受理装置の鍵配送用公開鍵を用いて共有鍵を生成し、
上記共有鍵で上記暗号化用鍵を暗号化して暗号化鍵の暗号化情報を生成し、
上記セキュリティ化証明書申請情報と、上記使い捨て公開鍵情報に上記暗号化鍵の暗号化情報を加えて証明書申請要求情報として上記申請受理装置へ送り、
上記セキュリティ化された情報の検証は、上記受け付けた上記証明書申請要求情報をセキュリティ化証明書申請情報暗号化用鍵の暗号化情報と使い捨て公開鍵情報とに分割し、
上記鍵配送用使い捨て公開鍵とその証明書申請受理装置の鍵配送用秘密鍵を用い共有鍵を生成し、
その共有鍵で上記暗号化用鍵の暗号化情報を復号化し、セキュリティ化証明書申請情報を上記共有鍵で復号して証明書申請情報とディジタル署名を取得し、上記ディジタル署名用使い捨て公開鍵を用いて証明書申請情報の検証を行うことであることを特徴とする請求項１記載の証明書発行方法。

【請求項３】　上記使い捨て鍵は離散対数系非対称鍵暗号方式における秘密鍵、公開鍵の対からなる鍵配送用使い捨て鍵と、秘密鍵と公開鍵の対からなるディジタル署名用使い捨て鍵であり、

2

上記使い捨て公開鍵情報は、上記鍵配送用使い捨て公開鍵および上記ディジタル署名用使い捨て公開鍵であり、
上記鍵配送用使い捨て秘密鍵と上記証明書申請受理装置の鍵配送用公開鍵を用いて共有鍵を生成し、
上記証明書申請情報のセキュリティ化は、上記証明書申請情報に対して上記ディジタル署名用使い捨て秘密鍵でディジタル署名を行い、かつ、この署名付証明書申請情報を上記共有鍵で暗号化してセキュリティ化証明書申請情報を得ることであり、
上記セキュリティ化された情報の検証は、受け付けたセキュリティ化証明書申請情報と使い捨て公開鍵情報とを分割し、
上記公開鍵情報中の鍵配送用使い捨て公開鍵とその証明書受理装置の鍵配送用秘密鍵を用いて共有鍵を生成し、
その共有鍵で上記セキュリティ化証明書申請情報を復号化して、署名付証明書申請情報を得、
この署名付証明書申請情報を上記公開鍵情報中の署名用使い捨て公開鍵を用いて署名検証することであることを特徴とする請求項１記載の証明書発行方法。

【請求項４】　本人性を示す機密情報を有する利用者情報、利用者鍵情報などを含む証明書申請情報を作成する手段と、
ディジタル署名用の使い捨て秘密鍵と公開鍵を生成する手段と、
離散対数系非対称鍵暗号方式における鍵配送用の使い捨て秘密鍵と公開鍵を生成する手段と、
暗号化用鍵をランダムに生成する手段と、
上記鍵配送用の使い捨ての秘密鍵と証明書申請受理装置の鍵配送用公開鍵を用いて共有鍵を生成する手段と、
上記証明書申請情報を上記ディジタル署名用使い捨て秘密鍵を用いてディジタル署名を行う手段と、
上記ディジタル署名付証明書申請情報を上記暗号化鍵で暗号化してセキュリティ化証明書申請情報を生成する手段と、
上記暗号化鍵を上記共通鍵で暗号化して暗号化された暗号化鍵情報を得る手段と、
上記セキュリティ化証明書申請情報と、上記暗号化された暗号化鍵情報と、上記ディジタル署名用使い捨て公開鍵と、上記鍵配送用使い捨て公開鍵とを上記証明書申請受理装置へ送信する手段と、
上記各手段を順次処理させたり、記憶手段に対する読み書きなどを行う制御手段と、
上記処理に必要な情報を記憶する上記記憶手段と、
を具備する証明書申請装置。

【請求項５】　本人性を示す機密情報を有する利用者情報、利用者鍵情報などを含む証明書申請情報を作成する手段と、
ディジタル署名用の使い捨て秘密鍵と公開鍵を生成する

手段と、
離散対数系非対称鍵暗号方式における鍵配送用の使い捨て秘密鍵と公開鍵を生成する手段と、
上記鍵配送用の使い捨ての秘密鍵と証明書申請受理装置の鍵配送用公開鍵とを用いて共有鍵を生成する手段と、
上記証明書申請情報を上記ディジタル署名用使い捨て秘密鍵を用いてディジタル署名を行う手段と、
上記ディジタル署名付証明書申請情報を上記共有鍵で暗号化してセキュリティ化証明書申請情報を生成する手段と、
上記セキュリティ化証明書申請情報と、上記ディジタル署名用使い捨て公開鍵と、上記鍵配送用使い捨て公開鍵とを上記証明書申請受理装置へ送信する手段と、
上記各手段を順次処理させたり、記憶手段に対する読み書きなどを行う制御手段と、
上記処理に必要な情報を記憶する上記記憶手段と、
を具備する証明書申請装置。
【請求項６】　鍵配送用秘密鍵を生成する手段と、
証明書申請装置からの証明書申請要求情報を受信する手段と、
受信された証明書申請要求情報を、セキュリティ化証明書申請情報と、暗号化された暗号化鍵情報と、ディジタル署名用使い捨て公開鍵と、鍵配送用使い捨て公開鍵とに分割する手段と、
上記秘密鍵と上記鍵配送用使い捨て公開鍵とを用いて共有鍵を生成する手段と、
上記共有鍵で上記暗号化された暗号化鍵情報を復号化して暗号化鍵を得る手段と、
上記暗号化鍵で上記セキュリティ化証明書申請情報を復号化してディジタル署名付証明書申請情報を得る手段と、
上記ディジタル署名付証明書申請情報を、上記ディジタル署名用使い捨て公開鍵を用いて証明書申請情報を検証する手段と、
上記各手段を順次処理させ、記憶手段への読み書きなどを行う制御手段と、
上記処理に必要な情報を記憶する上記記憶手段と、
を具備する証明書申請受理装置。
【請求項７】　鍵配送用秘密鍵を生成する手段と、
証明書申請装置からの証明書申請要求情報を受信する手段と、
受信された証明書申請要求情報を、セキュリティ化証明書申請情報と、ディジタル署名用使い捨て公開鍵と、鍵配送用使い捨て公開鍵とに分割する手段と、
上記秘密鍵と上記鍵配送用使い捨て公開鍵とを用いて共有鍵を生成する手段と、
上記共有鍵で上記セキュリティ化証明書申請情報を復号化してディジタル署名付証明書申請情報を得る手段と、
上記ディジタル署名付証明書申請情報を、上記ディジタル署名用使い捨て公開鍵を用いて証明書申請情報を検証

する手段と、
上記各手段を順次処理させ、記憶手段への読み書きなどを行う制御手段と、
上記処理に必要な情報を記憶する上記記憶手段と、
を具備する証明書申請受理装置。
【請求項８】　上記署名検証に合格すると、上記証明書申請情報中の本人性を示す機密情報からその正当性を検証する手段と、
その正当性の検証に合格すると、その申請情報に応じた証明書を発行する手段とを備えることを特徴とする請求項６又は７記載の証明書申請情報受理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は電気通信システムや電子計算機等を利用して、電子的な証明書を申請し、これを検証して証明書を発行する方法、及びその装置に関する。
【０００２】
【従来の技術】各種プログラムデータ、各種データベースのデータなど各種の電子情報を取得することが考えられる。この場合供給するデータが第３者により取得されないように、公開鍵の本人のものであることを示す証明書をデータ供給者が受取り、その証明書内の公開鍵を用いて供給データを暗号化して提供し、その利用者のみが秘密に保持する秘密鍵でその供給された暗号化データを復号できるようにする。
【０００３】このような証明書を発行してもらうには、従来においては、証明書申請者の本人性の確認を行うためにはオフラインでの本人認証を行う必要が存在した。そのため、自動化・効率化が制限され、その処理に少なからぬ時間・コストを要する。上述のような問題を解決して、個人情報を漏洩することなくセキュリティが確保された確実な本人認証を実現している技術は確立されていない。
【０００４】
【発明が解決しようとする課題】オフラインでの本人認証と同様の安全性を有しながら、本人認証のオンライン化による証明書申請・発行処理の効率化・リアルタイム化を実現する方法及びその装置を提供することである。上述の従来技術でも記述したが、証明書申請・発行におけるオンラインでの本人認証を実現した技術は確立されていない。
【０００５】本人認証を行うためには、本人しか持ちえない情報（または物）を提示する必要がある。電子の世界で本人認証を実現するための技術としてディジタル署名方式が存在するがディジタル署名方式は鍵の与信の上に成り立つ。与信された鍵を保有していない者の本人性を認証することは困難である。そのため従来技術では、初めて鍵の与信を受ける際にオフラインでの本人認証を必要とし、コスト面や利便性等において問題が存在し

た。鍵の与信がされていない状態からオンラインで本人性を認証するには、本人しか知りえない情報を認証を受けたい相手に示せば良いのであるが、その際に第三者にその情報が漏洩する等の脅威が存在する。本人しか知りえない情報がセキュリティの確保された状態で伝達することができれば、オンラインでの本人認証も可能となる。

【０００６】この発明の目的は、証明書申請者と証明書発行者がオンラインで効率的に証明書申請・発行処理が実施できる証明書発行方法を提供するものである。この発明の別の目的は、証明書発行機関システムを低コストで実施できる証明書発行方法を提供することにある。この発明のさらに別の目的は、第三者によるなりすましの脅威を排除した安全な証明書発行処理が実施できる証明書発行方法を提供することにある。

【０００７】

【課題を解決するための手段】この発明の証明書発行方法は、使い捨て鍵という新しい概念を導入することにより安全に本人認証を行うための情報の送受を可能とし、証明書申請者は証明書発行者に対し申請者しか知りえない情報、例えば本人がクレジット金融の会員であって、本人とクレジット会社しか知り得ないクレジット番号と本人の氏名、住所などとを安全に提示することで鍵の与信がされていない状態においてオンラインでの確実な本人性の認証を保証し、確実な証明書発行を実施可能とする。

【０００８】証明書発行方法の処理は以下のステップで実施される。

ステップ１：証明書申請者は証明書申請装置に対し、一般には本人しか知り得ない情報を含む証明書申請情報を入力する。

ステップ２：証明書申請装置は使い捨て鍵を生成し、それを用い証明書申請情報のセキュリティ化を行う。

ステップ３：証明書申請装置は上記使い捨て鍵と対をなす使い捨て公開鍵情報とステップ２でセキュリティ化した情報を証明書申請受理装置に送る。

ステップ４：証明書申請受理装置は使い捨て公開鍵情報を用いセキュリティ化された情報を検証し、検証結果を証明書発行装置に送る。

ステップ５：証明書発行装置は検証結果に応じ、証明書申請情報の取り扱いを決定する。

ステップ６：証明書発行装置は証明書申請情報の正当性が確認された場合、証明書の発行を行い、正当性を確認できない場合は証明書の発行は行われない。

ステップ７：証明書発行装置は証明書発行手続きの結果を申請者に対し通知する。

【０００９】

【発明の実施の形態】以下、図面を用いてこの発明の実施例について詳しく説明する。図１にこの発明の方法が適用されるシステム構成の例を示す。証明書申請者が証

明書申請装置１１を用いて、証明書申請情報を作り、通信回線１２で接続された認証局装置１３内の証明書申請受理装置１４に送る。証明書申請受理装置１４は受信情報を検証し、その検証結果と証明書申請情報を証明書発行装置１５へ送る。証明書発行装置１５は、その検証結果と、証明書申請情報の検証に応じた結果を通信回線１２を通じて証明書申請装置１１へ送る。

【００１０】図２に証明書申請装置１１の機能構成例を示す。申請情報生成部２１、署名用鍵生成部２２、配送用鍵生成部２３、共通鍵生成部２４、暗号化鍵生成部２５、署名部２６、暗号化部２７，２８、公開鍵送信情報生成部２９、送出すべき情報を結合する結合部３１、外部へ情報を送信する送信部３２、外部からの情報を受信する受信部３３、各種情報を記憶する記憶部３４、各部を順次制御したり、記憶部３４に対する読み書きを行ったりする制御部３５、各種情報、指令などを入力するキーボードなどの入力手段３６などよりなる。これらは通常はマイクロプロセッサなどにより構成される。

【００１１】図３に証明書申請受理装置１４、証明書発行装置１５の各機能構成例を示す。証明書申請受理装置１４では、外部からの情報を受信する受信部４１、受信された情報を分割する分割部４２、配送用鍵生成部４３、共通鍵生成部４４、復号化部４５，４６、署名検証部４７、各種情報を記憶する記憶部４８、各部を順次制御したり、記憶部４８に対する読み書きなどを行う制御部４９などを備えている。

【００１２】証明書発行装置１５は正当性検証部５１、証明書発行部５２、外部へ情報を送出する送信部５３を備える。証明書申請受理装置１４と証明書発行装置１５とが場所的に離れている場合は、これら間で情報を送、受する送信部、受信部がそれぞれ設けられる。次に図２乃至図４を参照して証明書申請の手順を説明する。証明書申請人は、証明書申請受信装置１４に対し、鍵配送用使い捨て公開鍵Ｅｐ２を証明書申請装置１１を操作して、請求し、この請求を受けた証明書申請受信装置１４は、配送用鍵生成部４３にて配送用使い捨て秘密鍵Ｅｓ２、公開鍵Ｅｐ２を生成し、その秘密鍵Ｅｓ２を記憶部４８に一時記憶すると共に証明書発行装置１５の送信部５３を介して証明書申請装置１１へ送る。証明書申請装置１１は受信した証明書申請受理装置１４の配送用使い捨て公開鍵Ｅｐ２を記憶部３４に一時記憶する。この鍵配送用鍵Ｅｓ２，Ｅｐ２は離散対数系非対称鍵暗号方式に用いられるものである。

【００１３】先に、証明書申請装置１１は申請者の操作にもとずき、利用者情報、利用者鍵情報等からなる証明書申請情報ＣＲＩを申請情報生成部２１で構築し（Ｓ１）、鍵配送用使い捨て鍵として秘密鍵Ｅｓ１と公開鍵Ｅｐ１を配送用鍵生成部２３で生成し（Ｓ２）、ディジタル署名用使い捨て鍵として秘密鍵Ｓｓ１と公開鍵Ｓｐ１を署名用鍵生成部２２で生成する（Ｓ３）。この署名

7

用使い捨て鍵Ｓｓ１、Ｓｐ１は素因数分解系非対称鍵暗号方式における鍵、その他の暗号方式にある鍵でもよい。

【００１４】証明書申請情報ＣＲＩには本人性を示す機密性が要求される情報（例えばクレジット暗号）も含まれている。鍵配送用使い捨て鍵は以下の関係を持つ。

Ｅｐ１＝Ｅｓ１・Ｇ［ｐ］

ここでＧ［ｐ］は公開パラメータである。つまりこの鍵は離散対数系非対称鍵暗号方式に用いられるものである。

【００１５】証明書申請装置１１は証明書申請情報ＣＲＩに秘密鍵Ｓｓ１を用いて署名部２６で電子署名を行い、ディジタル署名付証明書申請情報ＣＲＩ－Ｓを生成する（Ｓ４）。一方暗号化鍵生成部２５から暗号化用鍵Ｅｒ をランダムに生成し（Ｓ５）、これを用いて署名付証明書申請情報ＣＲＩ－Ｓに対し暗号化部２７で暗号化を行いセキュリティ化証明書申請情報ＣＲＩ－Ｓ－Ｅを生成する（Ｓ６）。

8

＊【００１６】また鍵配送用使い捨て秘密鍵Ｅｓ－１と証明書申請受理装置１４の公開鍵Ｅｐ－２を用いて共通鍵生成部２４で共有鍵ＳＫ＝Ｅｓ－１・Ｅｐ－２を生成する（Ｓ７）。この共有鍵ＳＫはＳＫ＝Ｅｓ－２・Ｅｐ－１の関係を持っている。この共有鍵ＳＫを用いて暗号化部２８で暗号化用鍵Ｅｒ を暗号化して暗号化鍵の暗号化情報Ｅｒ －Ｅを得る（Ｓ８）。

【００１７】公開鍵Ｓｐ－１とＥｐ－１を含む使い捨て用公開鍵送信情報ＤＰＩを公開鍵送信情報生成部２９で生成する（Ｓ９）。この情報ＤＰＩはＳｐ－１とＥｐ－１の単なるビット結合ＤＰＩ＝Ｓｐ－１‖Ｅｐ－１でよい。ＣＲＩ－Ｓ－ＥとＥｒ －ＥとＤＰＩとを結合部３１でビット結合して証明書申請要求情報ＳＣＲＩを生成し（Ｓ１０）、この申請要求情報ＳＣＲＩを証明書申請受理装置１４に送信部３２から送信する（Ｓ１１）。

【００１８】申請要求情報ＳＣＲＩは以下の関係式を満たす。

＊

$$\begin{aligned} SCRI &= DPI \,\|\, CRI-S-E \,\|\, Er-E \\ &= DPI \,\|\, (enc(Er : CRI-S)) \,\|\, (enc(SK : Er)) \\ &= DPI \,\|\, (enc(Er : sig(Ss-1 : CRI))) \,\|\, (enc(SK : Er)) \end{aligned}$$

ここで‖は連結を意味し、ｅｎｃ（Ａ：Ｂ）はＢを、鍵Ａを用いて暗号化することを意味し、ｓｉｇ（Ａ：Ｂ）はＢを、鍵Ａを用い署名付与することを意味する。

証明書検証／発行

この発明の一実施例に係る証明書申請受理装置／発行装置動作手順を図５に示す。

【００１９】証明書申請受理装置１４は受信部４１で受け付けた申請要求情報ＳＣＲＩをＤＰＩとＣＲＩ－Ｓ－ＥとＥｒ －Ｅとに分割部４１で分割する（Ｓ１）。そのＤＰＩからＳｐＩとＥｐＩを得る。そのＳｐ－１と証明書申請受理装置１４の暗号化用秘密鍵Ｓｓ－２を用いて共有鍵ＳＫを共有鍵生成部４４で生成する（Ｓ２）。つまり共有鍵生成部４４ではＳＫ＝Ｅｓ２・Ｅｐ１を演算する。証明書申請受理装置１４で生成された共有鍵ＳＫと証明書申請装置１１で生成された共有鍵ＳＫは同一である。

【００２０】生成した共有鍵ＳＫを用いてＥｒ －Ｅを復号化部４５で復号化を行い、暗号化鍵Ｅｒ を得る（Ｓ３）。その暗号化鍵Ｅｒ によりＣＲＩ－Ｓ－Ｅを復号化部４６で復号化してＣＲＩ－Ｓを得る（Ｓ４）。署名検証部４７でＤＰＩ中のＳｐ１を用いてＣＲＩ－Ｓの検証を行う（Ｓ５）。その検証結果が異常である場合、改ざん等脅威の存在が明らかであるため証明書登録を中止し登録が不完了となった旨を証明書申請装置１１に、証明書発行部５２より送信部５３を通じて提示する（Ｓ６）。

【００２１】署名検証結果によりＣＲＩの正当性が保証される場合、ＣＲＩから本人性を示す機密性が要求されている情報、例えばクレジット番号を取得し、その情報により本人性のチェックを正当性検証部５１で行う（Ｓ７）。つまり例えばそのクレジット番号が本人が有するものであるかのチェックを行う。本人性が確認された場合、証明書の発行を証明書発行部５２で行い、正常に証明書発行処理が終了した旨を証明書申請装置１１に送信部５３により提示する（Ｓ８）。本人性が確認できない場合、証明書発行処理を中止し証明書発行が行われなかった旨を証明書発行部５２で送信部５３を介して証明書申請装置１１に提示する（Ｓ６）。

【００２２】上述においては暗号化鍵Ｅｒ をランダムに発生させて証明書申請情報署名ＣＲＩ－Ｓを暗号化したが、図２中で破線で示すようにこの暗号化鍵Ｅｒ の替りに共有鍵ＳＫでＣＲＩ－Ｓを暗号化してもよい。この場合は、図２で暗号化鍵生成部２５、暗号化部２８が省略され、従って証明書申請受理装置１４へはＣＲＩ－Ｓ－ＥとＤＰＩが送られ、Ｅｒ －Ｅは省略される。証明書申請受理装置１４では復号化部４５が省略され、共有鍵生成部４４で生成された共有鍵ＳＫにより復号化部４６でＣＲＩ－Ｓ－Ｅに対する復号化が行われる。上述において、証明書申請受理装置は証明書発行装置を兼ねていてもよい。

【００２３】

【発明の効果】以上述べたように、この発明では使い捨て鍵という新しい概念を導入することにより、また本人のみが知り得る本人性を示す機密情報を証明書申請情報

に含めることにより本人性の保証に対してセキュリティの確保を実現する。さらに、証明書申請装置、証明書発行装置の負担も軽減され、証明書発行処理に関するシステムコストも少ない。

【００２４】また、第三者によるなりすましの脅威を防止し安全な証明書発行処理を実現できる。

【図面の簡単な説明】

【図１】この発明方法が適用されるシステムの構成例を示すブロック図。

【図２】この発明による証明書申請装置の実施例の機能構成を示すブロック図。

【図３】この発明による証明書申請受理装置の実施例の機能構成を示すブロック図。

【図４】図２に示した証明書申請装置の動作手順の例を示す流れ図。

【図５】図３に示した証明書申請受理装置の動作手順の例を示す流れ図。

【図１】

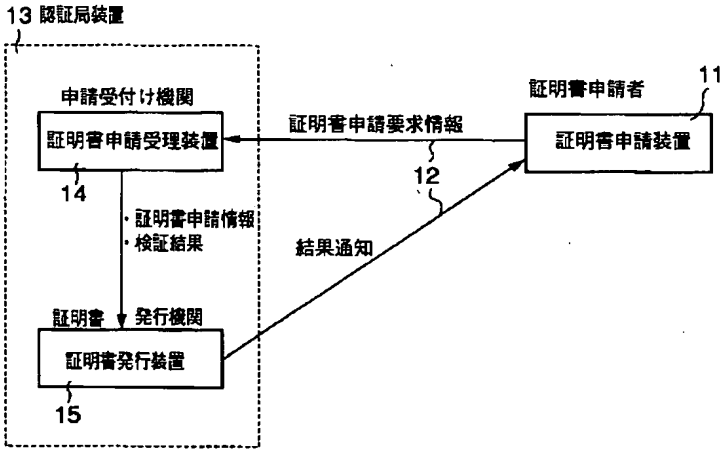

図 1

【図２】

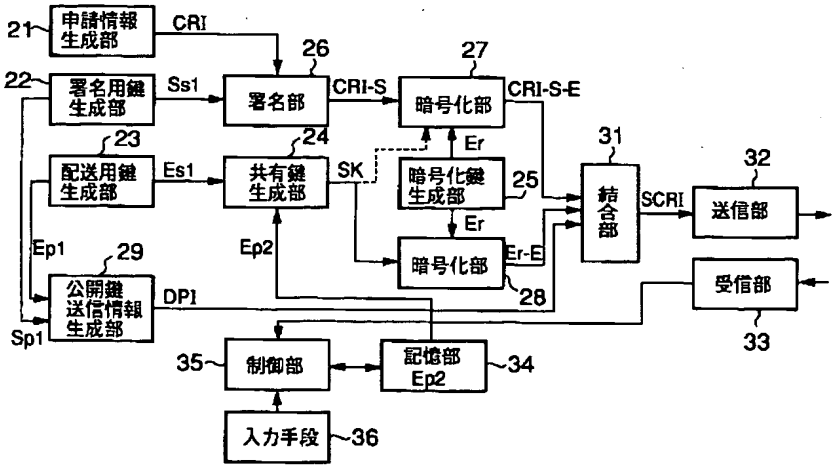

図 2

【図５】

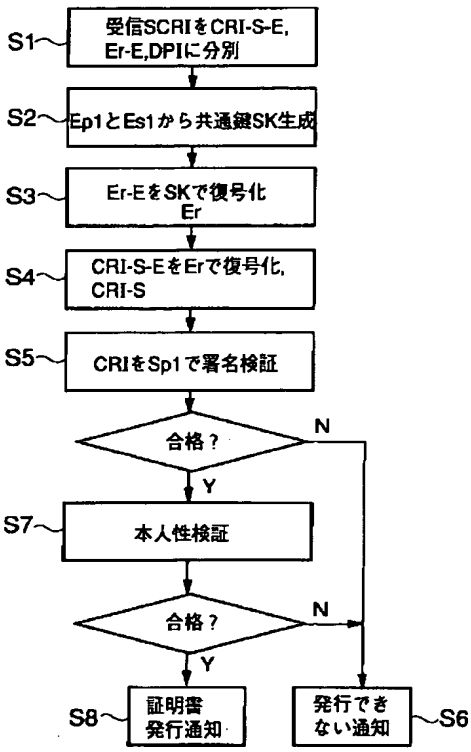

図 5

【図３】

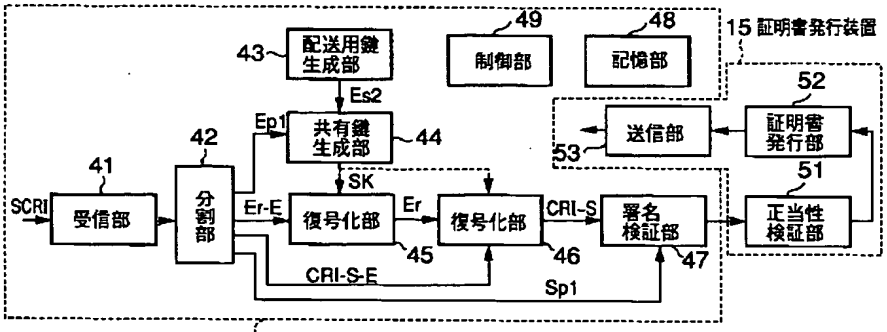

図 3

【図４】

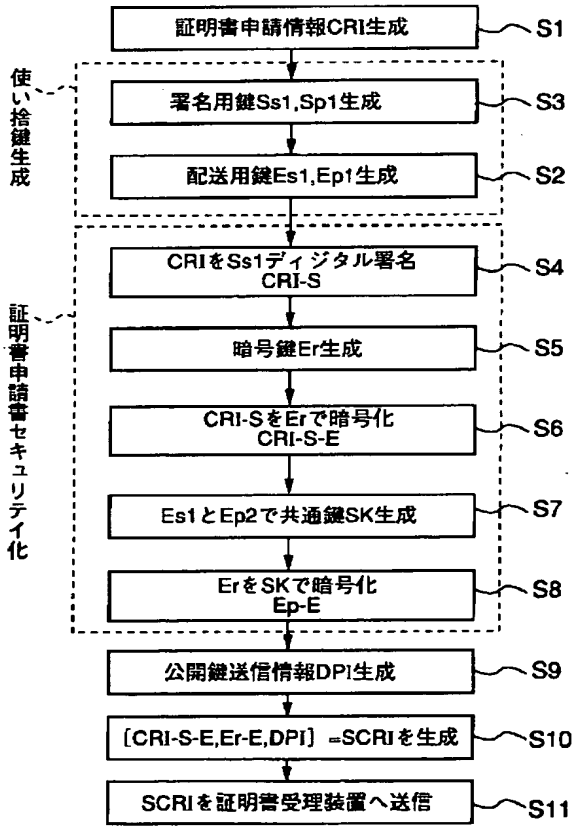

図 4

フロントページの続き

(72)発明者　安田　仁
東京都新宿区西新宿三丁目19番２号　日本
電信電話株式会社内